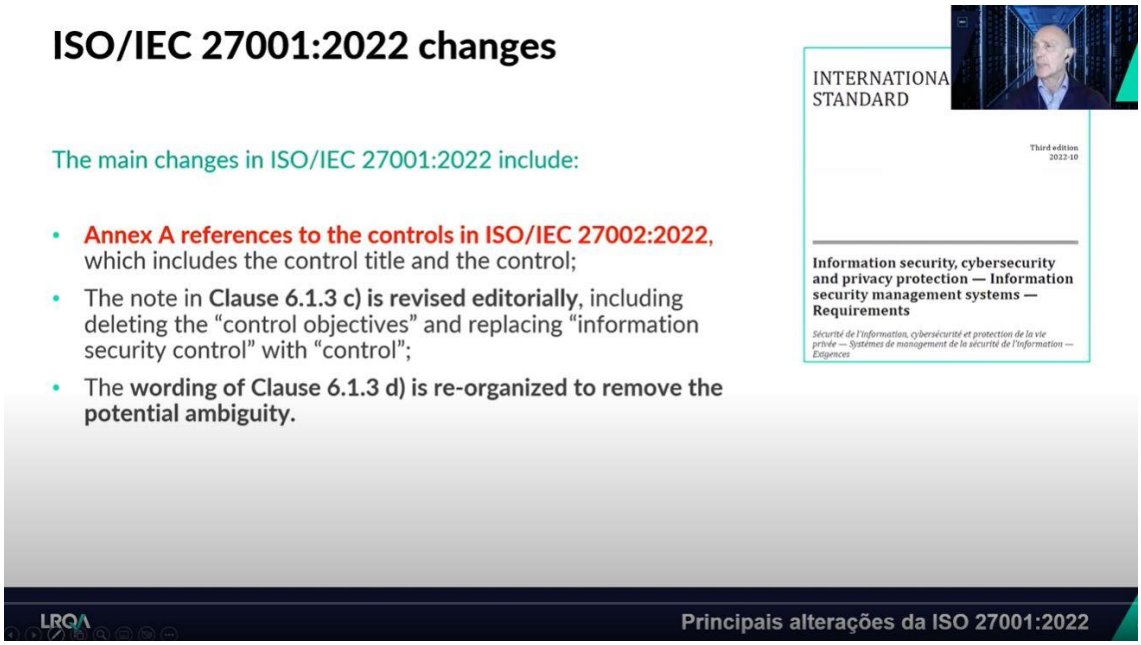
itSMF Portugal realiza sessão dedicada às principais alterações da nova ISO 27001:2022



No dia 23 de fevereiro realizou-se um It's Time To Talk About com Agustin Lerma, LRQA IT Technical Expert, South Europe. Durante uma hora foram apresentadas e discutidas com perguntas do público as principais alterações que traz a ISO 27001:2022.

ISO/IEC 27001: 2002 Alterações

As principais alterações à norma estão nas referências do Anexo A aos controlos na ISO/IEC 27002:2022, que inclui o título do controlo e o controlo propriamente dito; a nota da Cláusula 6.1.3 c) foi revista editorialmente, incluindo a exclusão dos "objetivos de controlo" e a substituição de "controlo de segurança da informação" por "controlo"; a redação da Cláusula 6.1.3 d) foi reorganizada, com a remoção de alguns termos e expressões, por forma a remover potenciais ângulos de ambiguidade. Cada organização tem, hoje, que dar conta de todos os controlos que aplica.

No total registam-se 11 novos controlos, 24 foram integrados entre si e 58 foram atualizados. Na verdade, a maioria das organizações cumpridoras já seguiam estes novos controlos. São eles:

5.7 Threat intelligence

5.23 Information security for use of cloud services

5.30 ICT readiness for business continuity

7.4 Physical security monitoring

8.9 Configuration management

8.10 Information deletion

8.11 Data masking

8.12 Data leakage prevention

8.16 Monitoring activities

8.23 Web filtering

8.28 Secure coding

Até aqui havia 114 controlos em 14 domínios e, com esta atualização, passa a haver 93 controlos em quatro domínios: organizacional (o que abarca mais recursos), de segurança física, das pessoas, e ao nível tecnológico.

A gestão de controlo do risco aplica-se à segurança da informação (física e ciber), serviços na *cloud*, data centers, de desenvolvimento de software, IoT Security, cripto, mobile e teletrabalho. "Este compêndio de assets dá-nos uma visão do que tem de ser implementado para proteger os ativos de informação", frisa Agustin Lerma.

Banca, energia, setor automóvel, jogos de azar, segurança nacional, saúde e telecomunicações estão entre os setores com os quais a LRQA mais tem trabalhado.

ISO/IEC 27001: Fase de transição

A principal recomendação que Agustin Lerma deixa passa por uma **revisão interna de cada organização sobre o seu atual processo de gestão de risco e qual a justificação para seleção ou não de determinados controlos com base no risco**. Serão auditados o design e implementação dos novos controlos.

A 25 de outubro de 2022 começou esta fase de transição que vai manter-se por três anos. A partir de novembro deste ano não serão mais emitidos certificados ISO/IEC 27001:2013 e os existentes vão perder a sua validade a 31 de outubro de 2025.

A LRQA espera começar a fazer certificação em ISO/IEC 27001:2022 a partir de 1 de maio próximo.

Perguntas e Respostas

Para quem quer começar a implementar um sistema de segurança da informação, como integrar a ISO 27001: 2022 com outras *frameworks* à volta?

Na cláusula 4 da norma estão as explicações do contexto. Sistemas internos e externos têm influência, como ter ou não *cloud*, ou em que país estou localizado, todos têm influência e essas *frameworks* têm de se ser integradas neste contexto. O especialista diz que "como auditor não posso esperar que quem começa tenha tudo perfeito. O importante é começar a fazer, sem receio de errar porque o objetivo é corrigir e melhorar".

A gestão da capacidade, tendo ficado no grupo tecnológico, só contempla os recursos dos sistemas de informação ou também os recursos humanos?

A gestão da capacidade tem de ser vista de forma transversal.

Um auditor cria valor e tem de perceber o nível de maturidade e análise de contexto da organização. Que desafios é que uma equipa de auditoria interna pode ter nesta fase de transição?

O auditor interno tem uma excelente oportunidade para levar a cabo a análise de onde está e para onde tem de caminhar a organização, identificando procedimentos que fazem parte do standard e fazendo uma leitura do plano de implementação.

Em que medida os atributos vêm realmente ajudar?

Vêm facilitar o processo proporcionando informação adicional que antes não existia. As pequenas empresas estão frequentemente desamparadas, com conhecimento limitado e necessitam de ajuda. O processo da gestão da mudança é o que tem o papel mais importante.

Temos de fazer a transição para a nova norma. Que sugestões de metodologia pode dar para realizar as alterações à ISO 27002:2022 que são necessárias e não podem ser realizadas em simultâneo?

Não há uma metodologia específica que possa recomendar-se, mas sim o criar de uma *checklist* e progressivamente trabalhar nela. Todos os dias estamos a aprender e atentos aos riscos que a IA e o *machine learning* estão a trazer.

Dia 23 de março há um novo It's Time To Talk About.